REMARKS

We have amended claims 1, 11, 14-18, 31, 38, and 47 to address the examiner's objection to informalities, and to more particularly point out and distinctly claim the invention. We have also added claim 48, and canceled claim 3. After entering the amendments identified herein, claims 1, 2, 4-20, 31, and 38-48 will be pending in the application.

The examiner rejected claims 1-4, 9-11, 14-17, 31, 33, 37-41, 43, and 47 under 35 U.S.C. §103(a) as being unpatentable over Jones (5,623,637) in combination with Shamir. The examiner argues that Jones discloses everything in the claims except for "a protocol wherein the client has a client secret and the server has a server secret used to compute a third secret from the client and server secret and the server cannot feasible determine the client secret of the third secret." The examiner argues that Shamir teaches that which is missing from Jones. We disagree. Shamir actually teaches less than what the examiner believes. Specifically, Shamir does not teach a protocol that is "implemented so that the client cannot feasibly determine the server secret and the server cannot feasibly determine the client secret or the third secret," as is recited in the independent claims 1, 38, and 47.

If we apply Jones to Shamir, there are first and second entities, e.g. a client and a server, who possess respective secrets D1 and D2, e.g. client and server secrets. Then either the first or second entity computes D, e.g. a third secret, from D1 and D2. However, contrary to the requirements of the claims, the secret sharing scheme disclosed by Shamir actually requires the first or second entity computing the secret to *simultaneously* know both D1 and D2 in order to feasibly compute D:

> Without loss of generality, we can assume that the data D is (or can be made) a number. To divide it into pieces Di, we pick a random k-1 degree polynomial $q(x) = a_0 + a_1x + \ldots a_{k-1}x^{k-1}$ in which a_0=D, and evaluate:
>
> D1=q(1), ..., Di=q(i), ..., Dn=q(n).
>
> Given any subset of k of these Di values (together with their identifying indeces), we can find the coefficients of q(x) by interpolation, and then evaluate D=q(0). Knowledge of just k-1 of these values, on the other hand, does not suffice in order to calculate D. (p. 613)

The first or second entity must know D1 *and* D2 (k=2) in order to compute D. Knowing only D1 *or* D2 (k=1) is not sufficient to compute D.

Therefore the first entity (e.g. the client) knowing D1, or the second entity (e.g. the server) knowing D2, *must be told the other entity's secret* in order to feasibly compute D (e.g. the third secret). The examiner correctly points out that if the server knows only D2 (k=1) then it cannot compute D. However, the examiner does not note that this then forces the client, knowing only D1, to *obtain* D2 (k=2) in order to compute D. If the client does not obtain D2 (k=1) then the client cannot feasibly compute D.

In other words, the secret sharing scheme disclosed by Shamir *requires* the client (having D1) to determine the server secret (D2) in order to calculate the third secret (D) *or requires* the server (having D2) to determine the client secret (D1) in order to calculate the third secret (D). Having only one of the client or server secrets is insufficient to compute the third secret. Thus the secret sharing scheme disclosed by Shamir violates the requirements of "a protocol [that] is implemented so that the client cannot feasibly determine the server secret and the server cannot feasibly determine the client secret or the third secret," as is recited in the independent claims.

None of the other art cited by the examiner supplies that which is missing from Jones and Shamir.

For the reasons stated above, we believe the claims are allowable and therefore ask the examiner to allow them to issue.

Dated: August 5, 2005

Respectfully submitted,

By _____

Eric L. Prahl
Registration No.: 32,590
WILMER CUTLER PICKERING HALE AND DORR LLP
60 State Street
Boston, Massachusetts 02109
(617) 526-6000
Attorney for Applicant